REMARKS

This amendment is a full and timely response to the non-final Office Action dated August 22, 2003. By this amendment, Applicants have amended claims 1 and 4 to recite a read history storage for storing said read history information and executing a control program when instructed by the external computer said collator begins collating when an instruction is received from the external processor. Moreover, claim 2 was amended to recite said registered fingerprint information includes a fingerprint template that corresponds to an owner of the external storage medium. Still further, by this amendment Applicants have added claims 5-18 to the instant application. Support for the changes to claims 1, 2, and 4, and newly added claims 5-18 can be found variously throughout the specification. For example, the changes to claims 1 and 4 can be found at page 4, lines 10-14 of the substitute specification. In addition, the changes to claim 2 can be found in the substitute specification at page 7, lines 18-21. In another example, support for newly added claims 5-18, and original claims 1-4 can be found in the substitute specification at page 6, line 1 through page 7, line 16. No new matter has been added. Claims 1-18 are pending where claims 1, 4, 5, 10, and 14 are independent.

Claim Objections

Claim 4 was objected to for alleged informalities. Applicants have amended claim 4 to recite, among other things, storing said read history information in read history storing means. Thus, Applicants respectfully request that the objection to claim 4 be withdrawn.

Rejections Under 35 U.S.C. § 102

Claims 1, 3, and 4 were rejected under 35 U.S.C. § 102(e) as anticipated by *Haneda et al.*, U.S. Patent No. 6,490,366. Applicants respectfully traverse this rejection.

Independent claim 1 recites a fingerprint collating device for collating a user's fingerprint with registered fingerprint information to effect personal authentication, said device comprising an external computer; a fingerprint reader for reading said fingerprint to create read fingerprint information, and to create read history information indicating that said read fingerprint information has been created; a read history storage for storing said read history information and executing a control program when instructed by the external computer; and a collator collating

said read fingerprint information with said registered fingerprint information to effect personal authentication and output a result of authentication when said read history information is stored in said read history storage and the control program is executed.

Independent claim 4 a fingerprint collating method for collating a user's fingerprint with registered fingerprint information to effect personal authentication, said method comprising the steps of reading said fingerprint to create read fingerprint information, and to create read history information indicating that said read fingerprint information has been created; storing said read history information in read hysteresis storing means; executing a control program in said read history storing means when an instruction signal is received from an external computer; and collating said read fingerprint information with said registered fingerprint information to effect personal authentication and output a result of authentication when said read history information is stored in said read history storing means and said read history storing means executes the control program.

As it relates to claims 1 and 4, the present invention is directed to a fingerprint collating device to prevent illicit use and unauthorized access to personal information. As is commonly known, collating involves a minute and critical inspection in order to note points of agreement or divergence. The fingerprint collating device, which is connected to a computer, includes a fingerprint reader, read history storage, and a collator. The fingerprint reader reads the fingerprint of a user and creates a fingerprint image. Moreover, the fingerprint reader generates read history information, which indicates that the fingerprint image has been created. The read history storage stores the read history information and executes a control program to perform a collating or comparative operation. The control program is executed based on an instruction from the computer. The computer sends the instruction to the read history storage when the read history storage stores the read history information. The collator then performs the minute and critical inspection of the fingerprint image with respect to the registered fingerprint information to note points of agreement or divergence based on the control program. Once this process is completed, the collator outputs an authentication result to the computer.

Haneda discloses an information processing apparatus that identifies a user by verifying the user's fingerprint. To verify a fingerprint, the user places his finger on a fingerprint detection section 6 or 15, and when a shadow of the finger is detected a backlight of detecting section 6 or

15 is turned on. The fingerprint is then detected and collated with previously stored fingerprint data. If the user's fingerprint coincides with the previously stored fingerprint data then the device power is turned on. In detecting the placement of the finger on detection section 6, the reflected light detected by sensor portion 62 is captured, stored in sensory memory 20, and outputted to a distribution operation section 21 to determine data distribution. Based on the data distribution of the captured image, the device determines whether a finger is placed on the fingerprint detecting section 6 by comparing the captured image to a distribution pattern stored in a distribution pattern detecting section 22. The distribution operation section 21 outputs a signal to a driving section 27, so that the backlight 6-3 is turned on, and outputs a signal to collating section 23 to drive collation. In addition, the distribution patter detecting section 22 outputs a signal to gate 29. A fingerprint storage flag 25-3 of a central section 25 indicates whether fingerprint information is stored in the fingerprint information storage section 24. When the fingerprint storage flag is set to "1," fingerprint information is stored in the fingerprint information storage section 24. The distribution pattern detecting section 22 also outputs a signal to collating section 23 to begin the collating process. When power is turned on the central control section 25 determines whether a secret mode is released, and if so, the fingerprint is detected based on the data of sensory memory 20 inputted from collating section 23, and the fingerprint is collated with a fingerprint previously stored in a fingerprint information storage section. *Haneda*, however, does not disclose, teach, or suggest that the read history storage section executes a control program when instructed by the external processor. Thus, it follows that *Haneda* further fails to disclose, teach, or suggest collating said read fingerprint information with said registered fingerprint information to effect personal authentication and output a result of authentication when said read history information is stored in said read history storage and the control program is executed. Instead, *Haneda* teaches that the fingerprint storage flag 25-3, is used a mechanism for powering the central control section 25 on or off.

As noted above, each of claims 1 and 4 recite, among other things, executing a control program in said read history storing means when an instruction signal is received from an external computer. *Haneda* fails to disclose, teach, or suggest at least this claim element. To properly anticipate a claim, the document must disclose, explicitly or implicitly, each and every feature recited in the claim. *See* Verdegall Bros. v. Union Oil Co. of Calif., 814 F.2d 628, 631, 2

USPQ2d 1051, 1053 (Fed. Cir. 1987). For at least the reasons discussed above, Applicants respectfully request that the rejection of claims 1 and 4 be withdrawn, and these claims be allowed.

Claim 3 depends from claim 1. By virtue of this dependency, Applicants submit that claim 3 is allowable for at least the same reasons given above with respect to claim 1. In addition, Applicants submit that claim 3 is further distinguished over *Haneda* by the additional elements recited therein, and particularly with respect to the claimed combination. Applicants respectfully request, therefore, that the rejection of claim 3 under 35 U.S.C. §102 be withdrawn, and this claim be allowed.

Claim 2 was rejected under 35 U.S.C. §102(e) as anticipated by *Senior*, U.S. Patent No. 6,400,836. Applicants respectfully traverse this rejection.

Claim 2 depends from claim 1, and additionally recites said collator effects said personal authentication by using said registered fingerprint information supplied from an external storage medium, wherein said registered fingerprint information includes a fingerprint template that corresponds to an owner of the external storage medium.

Senior discloses a fingerprint acquisition device scans a fingerprint image and saves the fingerprint in memory located in the device or in a computer. An extraction process is then performed on the fingerprint features to authenticate the scanned fingerprint. The extracted features are compared with stored fingerprint characteristics of authorized users. The stored fingerprint characteristics are maintained in a database. The acquisition device then determines whether the scanned fingerprint matches one of the fingerprints stored in the database. The result of the determination is expressed as a status flag. *See* col. 8, lines 36-65. *Senior* further discloses that fingerprint data can be contained in a removable device such as a smart card. *See* col. 10, lines 63-65. *Senior*, however, fails to disclose, teach, or suggest at least executing a control program as recited base claim 1. In fact, it appears that *Senior* does not disclose, teach, or suggest the creation of read history information. At col. 8, lines 52-65, *Senior* merely discloses that the scanned fingerprint and the stored fingerprint have been compared.

By virtue of the dependency for claim 1, claim 2 recites executing a control program in said read history storing means when an instruction signal is received from an external processor

and collating said read fingerprint information with said registered fingerprint information to effect personal authentication and output a result of authentication when said read history information is stored in said read history storage and the control program is executed. *Senior* fails to disclose, teach, or suggest at least these claim elements. To properly anticipate a claim, the document must disclose, explicitly or implicitly, each and every feature recited in the claim. *See* Verdegall Bros. v. Union Oil Co. of Calif., 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). For at least these reasons, Applicants respectfully request that the rejection of claim 2 under 35 U.S.C. § 102 be withdrawn, and this claim be allowed.

Newly Added Claims

As noted above, Applicants have added claims 5-18 to the instant application. Each of claims 5-18 recite, among other things, collating the fingerprint image of the user with the fingerprint template when a fingerprint accepting flag is set in the first memory unit. Because none of the prior art of record in the instant application discloses, teaches, or suggests at least this claim element, Applicants submit that claims 5-18 are allowable. Thus, Applicants respectfully request that the Examiner consider and allow these claims.

Conclusion

Based on at least the foregoing amendments and remarks, Applicants submit that claims 1-18 are allowable, and this application is in condition for allowance. Accordingly, Applicants request favorable reexamination and reconsideration of the application. In the event the Examiner has any comments or suggestions for placing the application in even better form, Applicants request that the Examiner contact the undersigned attorney at the number listed below.

Dated: October 17, 2003

Respectfully submitted,

By_____
Ronald P. Kananen
Registration No.: 24,104
Attorneys for Applicant

RADER, FISHMAN & GRAUER, PLLC
Lion Building
1233 20th Street, N.W., Suite 501
Washington, D.C. 20036
Tel: (202) 955-3750
Fax: (202) 955-3751
Customer No. 23353

DC135452

In the event additional fees are necessary in connection with the filing of this paper, or if a petition for extension of time is required for timely acceptance of same, the Commissioner is hereby authorized to charge Deposit Account No. 180013 for any such fees; and applicants hereby petition for any needed extension of time.